UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,526	08/16/2001	Arindam Das-Purkayastha	B-4274 618998-3	3735

			EXAMINER
36716	7590	09/16/2005	CHAI, LONGBIT

LADAS & PARRY
5670 WILSHIRE BOULEVARD, SUITE 2100
LOS ANGELES, CA 90036-5679

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/931,526	DAS-PURKAYASTHA ET AL.
	Examiner	**Art Unit**	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _04 August 2005_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-61_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _16 August 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is in response to the Appeal Brief filed on August 4, 2005. Claims 1 –

6 were originally received for consideration. Per the amendment received on December

14, 2004, new claims 7 – 61 were added and the claims 1 – 6 as pending in the

application. Claims 1 – 61 are currently being considered and the restriction

requirement has been withdrawn.

Response to Arguments

2.   In view of the Appeal Brief filed on August 4, 2005, PROSECUTION IS HEREBY

REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the

following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply

under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a

supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or

1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

1.   Claims 1 – 19, 22 – 37, 42 – 55 and 60 – 61 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Grawrock (Patent Number: 6678833), in view of Saunders

(Patent Number: 6209099), and in view of CCIMB-99-031 ("Common Criteria for

Information Technology Security Evaluation", August.1999 Version 2.1).

As per claim 42, Grawrock teaches a method for establishing communications

between a computer entity and a user, comprising:

presenting a request from the user to a trusted device associated with a

computer entity to provide an integrity metric calculated for the entity by the trusted

device and containing values indicative of one or more characteristics of the entity

(Grawrock: Column 4 Line 10 – 12 and Column 4 Line 35 – 40);

Examiner notes Grawrock teaches using the Trust Platform Module (TPM) as the

trusted 3rd party to provide target information metrics for verification by the trusted

device either internally or externally (Grawrock: Column 4 Line 10 – 12 and Column 4

Line 35 – 40). However, Grawrock does not disclose explicitly about that particular

trusted device.

Saunders teaches the use of security ASIC as the trusted device (Saunders: Figure 1 Element 15, Figure 2, Column 2 Line 42 – 46, Column 1 Line 43 – 50, Column 1 Line 14 – 17 and Column 3 Line 1 – 5).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Saunders within the system of Grawrock because Saunders providing an effective method and system for testing one or more components of a data processing system in order to determine the authenticity of the tested component or components (Saunders: Column 1 Line 30 – 34).

presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device (Saunders: Column 3 Line 47 – 50: the system and user as a whole is considered as a complete computer entity);

comparing at the user values in the integrity metric calculated for the entity by the trusted device (Saunders: Column 3 Line 47 – 50) with authenticated values provided for the entity by a trusted party (Grawrock: Column 4 Line 36 – 40 and Column 3 Line 65 – 67: TPM is the trusted 3rd party); and

Grawrock as modified does not teach selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device.

CCIMB-99-031 teaches selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device (CCIMB-99-031: Page 14 3rd Para, Page 15 1st Para, Page 41 Last Para and Page 48 Last Para).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of CCIMB-99-031 within the system of Grawrock as modified because CCIMB-99-031 teaches the prevention of system tampering by assigning a trusted assurance rating of the countermeasures, which gives grounds for confidence in their proper characteristics (CCIMB-99-031: Page 15 1st Para).

As per claim 1, 6, 7 and 24, the claim limitations are met as the same reasons as that set forth in rejecting claim 42.

As per claim 2, Grawrock as modified further teaches the trusted device is arranged to acquire an integrity metric of the computer entity (Grawrock: Column 3 Line 62 – Column 4 Line 9).

As per claim 3, Grawrock as modified does not teach the trust level is determined by comparing the value of the at least one characteristics with a specified value.

Trostle teaches the trust level is determined by comparing the value of the at least one characteristics with a specified value (Grawrock: Column 4 Line 6 – 9 and CCIMB-99-031: Page15 1st Para: assigns an assurance rating of the countermeasures, where the countermeasures are the verification results of a plurality of metrics as taught by Grawrock).

As per claim 4, Grawrock as modified further teaches the plurality of trust levels are determined base upon a plurality of specified values associated with a plurality of characteristics of a computer entity (Grawrock: Column 4 Line 6 – 9).

As per claim 5, Grawrock as modified further teaches the plurality of trust levels are determined based upon a plurality of specified values associated with characteristics for a plurality of computer entities (Grawrock: Column 4 Line 6 – 9 and CCIMB-99-031: Page15 1st Para: assigns an assurance rating of the countermeasures, where the countermeasures are the verification results of a plurality of metrics as taught by Grawrock).

As per claim 8, 25 and 43, Grawrock as modified further teaches the trusted device is hardwired to the computer entity (Saunders: Figure 1 Element 15).

As per claim 9, 26 and 44, Grawrock as modified further teaches the trusted device is configured to control the boot process of the computer entity (Saunders: Figure 3 Element 38 / 39 / 40).

As per claim 10, 27 and 45, Grawrock as modified further teaches the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device (Saunders:

Figure 3 Element 28: no further response from the trusted device if the boot key is not

entered and configured).

As per claim 11, 28 and 46, Grawrock as modified further teaches the trusted

device is comprised of a plurality of components hardwired to the computer entity

(Saunders: Column 2 Line 42 – 45).

As per claim 12, 29 and 47, Grawrock as modified further teaches the trusted

device is configured to contain one or more of a public encryption key, a private

encryption key, and one or more authenticated values provided for the entity integrity

metric by the trusted party (Saunders: Column 3 Line 36 – 38; Grawrock: Column 4 Line

15 – 18).

As per claim 13, 30 and 48, Grawrock as modified further teaches the trusted

device is configured to calculate the integrity metric by generating a digest of BIOS

instructions in the BIOS memory of the entity (Saunders: Figure 3 Element 38 / 39 / 40).

As per claim 14, 31 and 49, Grawrock as modified further teaches the trusted

device is configured to calculate the integrity metric by measuring one or more values of

configuration information regarding one or more components of the entity (Saunders:

Column 2 Line 42 – 45).

As per claim 15, 32, 36, 50 and 54, Grawrock as modified further teaches the

components of the entity are selected from among the group of components comprising

hardware components and software components (Saunders: Column 2 Line 42 – 45;

Grawrock: Column 4 Line 1 – 6).

As per claim 16, 33 and 51, Grawrock as modified further teaches wherein the

components of the entity are selected from among the group of components comprising

the BIOS, ROM, operating system loader, and operating system of the entity (Grawrock:

Column 4 Line 3 – 6).

As per claim 17, 34 and 52, Grawrock as modified further teaches the

configuration information measured for at least one of the components comprises one

or more of certificate information, last update information, latest update version

information, and previous update information (Grawrock: Column 4 Line 15 – 18).

As per claim 18, 35 and 53, Grawrock as modified further teaches the trusted

device is configured to calculate the integrity metric by engaging in predetermined

interactions with one or more components of the entity and acquiring the values of the

responses of the one or more components (Saunders: Column 1 Line 43 – 50).

As per claim 19, 37 and 55, Grawrock as modified further teaches the response received from the trusted device includes the authenticated values provided by the trusted party (Grawrock: Column 4 Line 35 – 40).

As per claim 22 and 60, Grawrock as modified further teaches initiating data transfer to the entity in accordance with the selected trust level (CCIMB-99-031: Page 48 Last para; Saunders: Column 3 Line 39: if the trust level is not accountable (i.e. invalid verification), the entire process is stop).

As per claim 23 and 61, Grawrock as modified further teaches initiating data transfer to the entity in accordance with the selected trust level comprises transferring no data (CCIMB-99-031: Page 48 Last para; Saunders: Column 3 Line 39: if the trust level is not accountable (i.e. invalid verification), the entire process is stop).

2.   Claims 20 – 21, 38 – 39, 40 – 41 and 56 – 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock (Patent Number: 6678833), in view of Saunders (Patent Number: 6209099), in view of CCIMB-99-031 ("Common Criteria for Information Technology Security Evaluation", August.1999 Version 2.1), and in view of Stoltz (Patent Number: 6615264).

As per claim 20, 38 and 56, Grawrock as modified does not disclose expressly generating a nonce to pass to the trusted device with the request.

Stoltz teaches generating a nonce to pass to the trusted device with the request

(Stoltz: Column 17 Line 64 – 66 and Column 18 Line 1 – 5: nonce is a random number).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Stoltz within the system of Grawrock as

modified because Stoltz teaches a security enhanced method to authenticate the

request for secure information either in a standalone computer system, in any other

computer systems or in a client-server system (Stoltz: Column 3 Line 65 – Column 4

Line 2, Column 4 Line 9 – 12, Column 17 Line 64 – 66 and Column 18 Line 1 – 5).

As per claim 21, 39 and 57, Grawrock as modified further teaches the response

from the trusted device includes the nonce received with the request (Stoltz: Column 18

Line 46 – 47).

As per claim 40 and 58, Grawrock as modified does not disclose expressly the

request includes input data.

Stoltz teaches the request includes input data (Stoltz: Column 17 Line 64 – 66

and Column 18 Line 1 – 5: random number is included as part of the request). See the

same rationale address above in rejection claim 20.

As per claim 41 and 59, Grawrock as modified teaches the response includes the

input data processed with the private encryption key (Stoltz: Column 17 Line 64 – 66,

Column 18 Line 1 – 5 and Column 2 Line 33 – 34: the request / response message is

encrypted).

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Longbit Chai whose telephone number is 571-272-3788.

The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100